ENDLICHE GRUPPEN, DEREN KOMMUTATORGRUPPENORDNUNG EINE PRIMZAHL $p \neq 2$ IST

INAUGURALDISSERTATION
ZUR ERLANGUNG DES DOKTORGRADES
GENEHMIGT VON DER
MATHEMATISCH-NATURWISSENSCHAFTLICHEN FAKULTÄT
DER FRIEDRICH-WILHELMS-UNIVERSITÄT
ZU BERLIN

VON

HEINZ LIERMANN
AUS ALTLÜLFITZ (POMMERN)

TAG DER MÜNDLICHEN PRÜFUNG: 23. NOVEMBER 1938
TAG DER PROMOTION: 17. FEBRUAR 1939

DRUCK VON B. G. TEUBNER IN LEIPZIG

N 119

REFERENTEN:
DOZENT DR. F. NEISS
PROFESSOR DR. E. SCHMIDT

R. UNIV.
BIBLIOTHEEK
LEIDEN

Sonderabdruck aus den „Schriften des Mathematischen Instituts und des Instituts für angewandte Mathematik der Universität Berlin" / Band 4

Einleitung.

Die rein gruppentheoretischen Arbeiten kann man ihrem Ziele nach in zwei Klassen teilen. In der einen Klasse liegen alle jene Arbeiten, in denen Sätze und Relationen hergeleitet werden, die für alle Gruppen Gültigkeit besitzen. Ich erinnere hierbei an den JORDAN-HÖLDERschen Kettensatz und die allgemeinen Zerlegungssätze. Ihnen gegenüber stehen die Arbeiten, in denen nur spezielle Gruppen behandelt werden. Aus der Gesamtheit aller Gruppen wird eine Teilmenge, deren Gruppen durch eine gemeinsame Eigenschaft vor den übrigen ausgezeichnet sind, herausgegriffen. Das Ziel dieser Arbeiten ist dann, einen nach Möglichkeit vollkommenen Überblick über die Struktur dieser speziellen Gruppen zu geben. Als klassisches Beispiel führe ich die Untersuchungen über die endlichen abelschen Gruppen an. Die gemeinsame Eigenschaft ist hier das kommutative Gesetz der Gruppenelemente. Das Endergebnis ist der Hauptsatz über die abelschen Gruppen, der in der Tat einen vollkommenen Überblick über diese Gruppen gibt. Als zweites Beispiel erwähne ich die Untersuchungen über die HAMILTONschen Gruppen. Unter einer HAMILTONschen Gruppe versteht man eine nichtabelsche Gruppe, deren sämtliche Untergruppen invariant sind. Das Endergebnis dieser Untersuchungen kann folgendermaßen ausgesprochen werden:

Jede endliche HAMILTONsche Gruppe gestattet eine eindeutige Zerlegung

$$H = Q \times A \times U, \tag{1}$$

wobei Q die Quaternionengruppe, A eine abelsche Gruppe vom Typus $[2, 2, \ldots, 2]$ und U eine beliebige abelsche Gruppe von ungerader Ordnung ist.

Dieser Satz wurde 1932 im mathematischen Seminar in Halle bewiesen.[1]) Der Grund, weshalb man bei den abelschen Gruppen relativ leicht zum Ziel kommt, ist offenbar der, daß man wegen des kommutativen Gesetzes mit den Gruppenelementen so bequem rechnen kann. Geht man von den abelschen Gruppen zu den nichtabelschen über, so

1) Vgl. R. Baer, *Situation der Untergruppen und Struktur der Gruppe*. Sitzungsber. Akademie Heidelberg 1933, Nr. 2, S. 12—17.

treten als störende Faktoren die Kommutatorelemente auf, also Elemente der Form $A^{-1}B^{-1}AB = C$. Man wird vermuten, daß man eine Gruppe desto leichter wird übersehen können, je einfacher die Kommutatorgruppe gebaut ist. Die Kommutatorgruppe ist die kleinste Untergruppe, die sämtliche Kommutatorelemente enthält. Die Vermutung wird bestätigt durch die Untersuchungen über abelsche Gruppen, bei denen die Kommutatorgruppe ja nur aus dem Einselement besteht. Aber auch bei den HAMILTONschen Gruppen trifft die Vermutung zu; denn aus der Darstellung (1) der HAMILTONschen Gruppen erkennen wir, daß die Kommutatorgruppe einer HAMILTONschen Gruppe die Ordnung 2 hat. Nach den endlichen abelschen Gruppen wird man also als nächst einfachere Gruppenart alle die endlichen Gruppen ansehen, deren Kommutatorgruppenordnung eine Primzahl ist. Diese Gruppen werden für $p \neq 2$ in der vorliegenden Arbeit behandelt. Sie stellen einen Spezialfall der zweistufigen[2]) Gruppen dar. Die Untersuchung wird in zwei Schritten durchgeführt. Zuerst wird der Fall behandelt, daß die Kommutatorgruppe im Zentrum liegt. Das Endergebnis ist analog wie bei den Untersuchungen über endliche abelsche Gruppen die Kennzeichnung dieser Gruppen durch ein Schema invarianter Zahlen derart, daß jeder Gruppe genau ein Schema zugeordnet werden kann und umgekehrt zu jedem Zahlenschema genau eine Gruppe gehört. Jedoch weist dieses Zahlenschema gegenüber dem bei abelschen Gruppen insofern etwas ganz Neuartiges auf, als es eine innere Struktur besitzt. Es kommt nämlich bei ihm nicht nur auf die invarianten Zahlen allein an, sondern auch auf ihre Beziehungen untereinander. So treten hier die Zahlen z. B. in Paaren auf, und diese Paarung ist durchaus wesentlich für die Struktur der Gruppe und durch diese eindeutig bestimmt. Außerdem sind die Invarianten nicht untereinander gleichwertig. So ist z. B. in unserem Falle *eine* Invariante durch Unterstreichung vor den anderen ausgezeichnet. Sie kennzeichnet hier die Lage der Kommutatorgruppe in der Gesamtgruppe und ist umgekehrt dadurch eindeutig festgelegt. Auch die Stellung im Schema kann wesentlich für die Struktur der Gruppe sein. Es ist ja letzten Endes nicht erstaunlich, daß man durch wenige strukturlose Zahlenschemata nicht der komplizierten inneren Struktur einer Gruppe gerecht

2) Vgl. A. Scholz, *Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe.* Math. Zeitschr. 30 (1929), S. 332—356; *Ein Beitrag zur Theorie der Zusammensetzung endlicher Gruppen.* Ebda. 32 (1930), S. 187—189; *Die Behandlung der zweistufigen Gruppe als Operatorengruppe.* Sitzungsber. Akademie Heidelberg 1933, Nr. 2, S. 17—22.

werden kann. Bestätigt wird dies z. B. durch die Untersuchungen von HOPKINS.[3])

Die Arbeit von HOPKINS behandelt allgemein Gruppen, deren Kommutatorgruppe im Zentrum liegt. Man gelangt hierbei schließlich zu acht Schemata invarianter Zahlen. Aber sie reichen dennoch nicht aus zur eindeutigen Kennzeichnung der Gruppen. HOPKINS sagt hierzu[4]): "For certain small values of m (for $m = 3$ and $m = 4$, in particular) these eight invariants characterize G. It would be an interesting problem to determine whether for every order of G there exists a set of arithmetical invariants which completely characterize G: that is, determine G to within an isomorphism."

Liegt die Kommutatorgruppe nicht im Zentrum, so ist die Struktur der Gruppe eindeutig bestimmt durch die Struktur des Zentrums und der Faktorgruppe nach dem Kommutator. Die Ergebnisse des ersten Teiles von § 1 sind nach einer mündlichen Mitteilung bei Herrn A. SCHOLZ a. a. O. [2]) enthalten und können dort durch Spezialisierung gewonnen werden.

§ 1. Endliche Gruppen, deren Kommutatorgruppenordnung eine Primzahl ist und deren Kommutatorgruppe im Zentrum liegt.[5])

Die Gruppen bezeichne ich in der Arbeit mit großen deutschen Buchstaben, die Elemente mit großen lateinischen Buchstaben und die Ordnungen mit kleinen lateinischen Buchstaben.

Die Kommutatorgruppe $\mathfrak{C}$ der zu untersuchenden Gruppe $\mathfrak{M}$ ist nach Voraussetzung zyklisch, kann also durch ein Element C erzeugt werden: $\mathfrak{C} = (C)$. Außerdem liegt $\mathfrak{C}$ nach Voraussetzung im Zentrum $\mathfrak{Z}$, also $\mathfrak{C} \leqq \mathfrak{Z}$. Die Ordnung von C ist eine Primzahl p, mithin wird $C^p = E$. Die Faktorgruppe $\mathfrak{M}/\mathfrak{C}$ ist abelsch.[6]) Sie sei vom Typus

$$[p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}].$$

3) C. Hopkins, *Metabelian groups of order p^m, $p > 2$.* Transactions Amer. Math. Soc. 37 (1935), S. 161—195.

4) A. a. O. [3]), S. 173.

5) Vgl. A. Scholz, *Reduktion der Konstruktion von Körpern mit zweistufiger (metabelscher) Gruppe* (Beiträge zur Algebra 14). Sitzungsber. Akademie Heidelberg 1929, Nr. 14, S. 3—15. Herr Scholz behandelt dort die zweistufigen p-Gruppen. Er strebt dabei aber nicht wie ich eine eindeutige Darstellung, die eine Abzählung aller verschiedenen Gruppen ermöglicht, sondern eine Darstellung als relatives Produkt an.

6) Vgl. A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, 2. Aufl. Berlin 1927, S. 42, Satz 35.

A_i sei irgendein Repräsentant aus einer erzeugenden Restklasse des i-ten Faktors von $\mathfrak{M}/\mathfrak{C}$. Dann kann ich $\mathfrak{M}$ erzeugen durch die $s+1$ Elemente $A_1, A_2, \ldots, A_s$ und C mit Hilfe folgender definierender Relationen:

$$(2) \qquad \begin{cases} A_i^{p_i^{\alpha_i}} = C^{a_i}, & A_i A_k = A_k A_i C^{c_{ik}}, \\ A_i C = C A_i, & C^p = E \end{cases} \qquad (i, k = 1, 2, \ldots, s).$$

Es fragt sich: Welche notwendigen und hinreichenden Bedingungen müssen die Zahlen p_i, α_i, a_i, c_{ik}, p und s erfüllen, damit auch wirklich eine Gruppe entsteht? Es ist leicht zu zeigen, daß

$$(3) \qquad c_{ik} + c_{ki} \equiv 0 \pmod{p}$$

und

$$(4) \qquad c_{ik} p_k^{\alpha_k} \equiv 0 \pmod{p}$$

notwendige Bedingungen sind; denn es ist

$$A_k A_i = A_i A_k C^{c_{ki}},$$

woraus

$$A_i A_k = A_k A_i C^{-c_{ki}}$$

folgt; andererseits ist

$$A_i A_k = A_k A_i C^{c_{ik}},$$

also

$$c_{ik} \equiv -c_{ki} \pmod{p}.$$

Ferner ist

$$A_i A_k^2 = A_k A_i C^{c_{ik}} A_k = A_k A_i A_k C^{c_{ik}} = A_k^2 A_i C^{2c_{ik}}$$

oder für beliebiges n

$$A_i A_k^n = A_k^n A_i C^{nc_{ik}}.$$

Setzt man $n = p_k^{\alpha_k}$, so ist A_k^n wegen $A_k^n = C^{a_k}$ mit A_i vertauschbar, mithin muß gelten

$$c_{ik} p_k^{\alpha_k} \equiv 0 \pmod{p}.$$

Daß diese beiden Bedingungen (3) und (4) auch hinreichen, wird hier nicht bewiesen. Es folgt dies unmittelbar aus einem Satz von SCHREIER.[7])

Die Bedingung (3) besagt offenbar, daß die Matrix (c_{ik}) schiefsymmetrisch ist.

---

7) O. Schreier, *Über die Erweiterung von Gruppen* I. Monatshefte f. Math. u. Physik 34 (1926), S. 165—180.

Es ist

$$(A_i A_k)^3 = (A_i A_k)^2 A_i A_k = A_i^2 A_k^2 C^{c_{ki}} A_i A_k$$
$$= A_i^2 A_k^2 A_i A_k C^{c_{ki}} = A_i^3 A_k^3 C^{2c_{ki}+c_{ki}}$$

oder allgemein

$$(A_i A_k)^n = A_i^n A_k^n C^{c_{ki}(1+2+\cdots+n-1)} = A_i^n A_k^n C^{c_{ki}\frac{1}{2}n(n-1)}.$$

Für $n = p \neq 2$ ergibt sich daraus die wichtige Relation

$$(A_i A_k)^p = A_i^p A_k^p. \tag{5}$$

Wir setzen daher für die folgenden Untersuchungen voraus, daß p eine ungerade Primzahl ist. Die Relation (5) besagt, daß sich die behandelten Gruppen hinsichtlich aller Ordnungsrelationen genau so verhalten wie abelsche Gruppen, wovon im folgenden oft ohne besonderen Hinweis Gebrauch gemacht wird. Es erweist sich nämlich später, daß die Ordnung von $\mathfrak{M}$ als Potenz von p angenommen werden kann.

Möge ferner für zwei beliebige Elemente X und Y gelten $XY = YXC^z$, so ergibt sich nach (2)

$$X^p Y = Y X^p C^{pz} = Y X^p,$$

woraus das wichtige Ergebnis folgt:

Die p-te Potenz eines jeden Elementes liegt im Zentrum.

Jedes Gruppenelement M kann eindeutig in der Form

$$M = A_1^{x_1} A_2^{x_2} \ldots A_s^{x_s} C^y$$

dargestellt werden, wobei $x_i \bmod p_i^{\alpha_i}$ und $y \bmod p$ gerechnet werden. Die Eindeutigkeit der Darstellung ergibt sich, nachdem die A_i, die zunächst willkürlich herausgegriffene Repräsentanten waren, festgelegt sind, folgendermaßen: Wird die Gruppe $\mathfrak{M}$ in ihre Nebengruppen nach $\mathfrak{C}$ zerlegt, so kann jeder Komplex eindeutig in der Form

$$(A_1\mathfrak{C})^{x_1} (A_2\mathfrak{C})^{x_2} \cdots (A_s\mathfrak{C})^{x_s}$$

geschrieben werden, wobei es auf die Reihenfolge der $(A_i\mathfrak{C})^{x_i}$ nicht ankommt, da $\mathfrak{M}/\mathfrak{C}$ abelsch ist. Durchläuft x_i die Werte von 0 bis $p_i^{\alpha_i} - 1$, so erhält man jede Nebengruppe nach $\mathfrak{C}$ genau einmal. Nun ist

$$(A_1\mathfrak{C})^{x_1} (A_2\mathfrak{C})^{x_2} \cdots (A_s\mathfrak{C})^{x_s} = A_1^{x_1} A_2^{x_2} \cdots A_s^{x_s}\mathfrak{C},$$

auch hier ist noch Vertauschbarkeit der $A_i^{x_i}$ zulässig. Jedes Gruppenelement liegt bekanntlich in einer und nur einer Nebengruppe. Um

nun für die einzelnen Gruppenelemente eine eindeutige Darstellung zu gewinnen, muß ich eine bestimmte Reihenfolge der A_i vorgeben; danach ist jedes Gruppenelement M eindeutig in der Form

$$M = A_1^{x_1} A_2^{x_2} \cdots A_s^{x_s} C^y$$

darstellbar, wobei $x_i \bmod p_i^{\alpha_i}$ und $y \bmod p$ zu rechnen sind. Eine Vertauschung der A_i ändert nur die Zahl y, wovon später Gebrauch gemacht wird.

Ist ein Basiselement A_i mit allen übrigen Basiselementen A_k vertauschbar, d. h. ist $c_{ik} = 0$ für $k = 1, 2, \ldots, s$, so liegt A_i im Zentrum; denn mit C ist A_i nach Voraussetzung vertauschbar, und jedes Element von $\mathfrak{M}$ wird durch ein Produkt der A_k und C erhalten. Ist nun für ein solches A_i außerdem $(A_i) \supsetneqq (C)$, d. h. $a_i = 0$, so kann die durch A_i erzeugte zyklische Gruppe (A_i) direkt abgespalten werden; denn der übrige Bestandteil

$$\mathfrak{U}_i = (A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_s, C)$$

ist, da er die Kommutatorgruppe (C) enthält, ebenso wie (A_i) ein Normalteiler. Da die beiden Normalteiler (A_i) und $\mathfrak{U}_i$ wegen $a_i = 0$ teilerfremd zueinander sind, so ist ihr Produkt ein direktes, das mit der Gesamtgruppe $\mathfrak{M}$ identisch ist, weil es alle Erzeugenden enthält. Von Bedeutung ist diese Abspaltung für die Basiselemente A_k mit $p_k \neq p$. Aus der Bedingung (4) folgt nämlich für $p_k \neq p$, daß $c_{ik} \equiv 0 \pmod{p}$ für $i = 1, 2, \ldots, s$ ist. Es liegt also A_k und damit auch A_k^p im Zentrum. Weiter ist

$$(A_k^p)^{p_k^{\alpha_k}} = C^{p a_k} = E\,, \text{ also } (A_k^p) \supsetneqq (C)\,,$$

mithin kann die zyklische Gruppe (A_k^p) direkt abgespalten werden. Lassen wir nun alle diese Faktoren fort, so folgt unmittelbar, daß

$$\text{Ord } \mathfrak{M} = p^\mu$$

angenommen werden kann. Diese Tatsache folgt auch direkt aus einem Satz von BURNSIDE.[8]) Wir können also im Typus $[p_1, p_2, \ldots, p_s]$ von $\mathfrak{M}/\mathfrak{C}$ die Indizes löschen.

Unsere nächste Aufgabe wird es sein, zu untersuchen, welche Vereinfachungen in dem Zahlensystem der (c_{ik}) und a_i durch geeignete Wahl der Basis erzielt werden können.

Zum besseren Verständnis des folgenden Beweises gebe ich zunächst das Ergebnis an. Bei der vorzunehmenden Normierung der Basis

8) Eine Gruppe, deren Kommutatorgruppe im Zentrum liegt, zerfällt direkt in p-Gruppen.

kann erreicht werden, daß unter den Zahlen a_i höchstens eine gleich 1, alle anderen gleich 0 sind. Ist nun $a_m = 1$ und $a_i = 0$ für $i \neq m$, so enthält die normierte Basis ein ausgezeichnetes Element A_m, dessen p^{α_m}-te Potenz die Kommutatorgruppe erzeugt. Die anderen Basiselemente besitzen diese Eigenschaft nicht. In diesem Falle kommt man mit s Basiselementen bei der Darstellung eines jeden Elementes M aus, C wird entbehrlich, jedoch muß $x_m \bmod p^{\alpha_m+1}$ gerechnet werden. Je nachdem nun, ob dieses ausgezeichnete Element A_m im Zentrum liegt oder nicht, unterscheiden wir bei der folgenden Klassifizierung der Gruppen die beiden Fälle A. und B.

Sind alle $a_i = 0$, so wird C bei der Darstellung von M nicht entbehrlich. Es erweist sich als zweckmäßig, diese Gruppen unter den Fall A. zu rechnen.

Fall A. Nach der Normierung haben die übrigen Basiselemente außer A_m, das im Zentrum liegt, die Eigenschaft, daß sie nur genau mit einem von ihnen nicht vertauschbar sind. Die so normierte Basis wollen wir folgendermaßen bezeichnen: Das ausgezeichnete im Zentrum liegende Basiselement, von dem eine geeignete Potenz die Kommutatorgruppe erzeugt, sei D mit $D^{p^{\gamma-1}} = C$. Nun entspricht einem Basiselement R_1 genau ein mit ihm nicht vertauschbares Basiselement S_1, ebenso R_2 das Element S_2, ..., R_t das Element S_t. Demnach ist in diesem Falle die Anzahl der Basiselemente der normierten Basis $2t + 1$, also stets ungerade. Es ergeben sich danach die definierenden Relationen

$$R_i^{p^{\varrho_i}} = E,\ S_i^{p^{\sigma_i}} = E,\ D^{p^{\gamma-1}} = C,\ C^p = E,\ R_i S_i = S_i R_i C \quad (i = 1, 2, \ldots, t),$$

sonst kommutativ.

Im Spezialfall $\gamma = 1$ ist das Element D mit C identisch. Es tritt dann das die Kommutatorgruppe erzeugende Element C selbst unter den Elementen der normierten Basis auf. Es ist dies nach obigem der Fall, wenn alle $a_i = 0$ sind. Die Zahlenmatrix (c_{ik}) enthält in jeder Zeile und Spalte genau eine 1 oder -1, sonst nur Nullen mit Ausnahme einer Zeile und Spalte, die nur aus Nullen bestehen. Die Zahlen sind nach der Normierung sämtlich Null bis auf eine, die den Wert 1 hat. Wir können in diesem Falle A. in Analogie zur Kennzeichnung der endlichen abelschen Gruppen durch folgendes Zahlenschema charakterisieren:

$$\left[\begin{matrix}\varrho_1, \varrho_2, \ldots, \varrho_t \\ \sigma_1, \sigma_2, \ldots, \sigma_t\end{matrix}; \gamma\right]_p. \tag{6}$$

In diesem Schema können natürlich die Zahlenpaare $\left\{ \begin{matrix} \varrho_i \\ \sigma_i \end{matrix} \right\}$ beliebig vertauscht werden, ebenso kann innerhalb eines jeden Paares die Anordnung geändert werden, also $\left\{ \begin{matrix} \varrho_i \\ \sigma_i \end{matrix} \right\} = \left\{ \begin{matrix} \sigma_i \\ \varrho_i \end{matrix} \right\}$, ohne daß die Struktur der Gruppe sich ändert.

Fall B. In der normierten Basis gibt es für $i = 1, 2, \ldots, t$ zu jedem Basiselement R_i genau ein Basiselement S_i, das mit ihm nicht vertauschbar ist. Die Anzahl der erzeugenden Basiselemente ist dann $2t$, also gerade. Weiter hat die Basis die Eigenschaft, daß genau eine der $2t$ zyklischen Gruppen (R_i) und (S_i) die Kommutatorgruppe (C) enthält, etwa (S_m). Die die Gruppe definierenden Relationen sehen folgendermaßen aus:

$$R_i^{p^{\varrho_i}} = E,\ S_i^{p^{\sigma_i}} = E,\ S_m^{p^{\sigma_m - 1}} = C,\ R_i S_i = S_i R_i C \quad (i = 1, 2, \ldots, t),$$

sonst kommutativ.

Das die Gruppe kennzeichnende Zahlenschema hat dann die Gestalt

$$\left[\begin{matrix} \varrho_1, \varrho_2, \ldots, \varrho_{m-1}, \varrho_m, \varrho_{m+1}, \ldots, \varrho_t \\ \sigma_1, \sigma_2, \ldots, \sigma_{m-1}, \underline{\sigma_m}, \sigma_{m+1}, \ldots, \sigma_t \end{matrix} \right]_p . \tag{7}$$

Auch hier bestehen dieselben Umstellungsmöglichkeiten der Zahlen, wie sie im Fall A. angegeben worden sind. Wesentlich ist nur, daß die Zahlen eines jeden Paares zusammenbleiben.

Es ist nun im folgenden zu zeigen, daß die Basis stets in der angegebenen Weise normiert werden kann.

Zunächst transformiere ich die Basis so, daß höchstens eine der Zahlen a_i von Null verschieden ist. Das Basiselement A_m besitze unter allen Basiselementen A_i mit der Eigenschaft $a_i \neq 0$ die höchste Ordnung. Gibt es kein solches A_m, d. h. sind von Anfang an alle $a_i = 0$, so liegt der oben bei A. erwähnte Spezialfall $\gamma = 1$ vor. Man ist dann schon fertig. Andernfalls wähle man an Stelle eines jeden Elementes A_i mit $a_i \neq 0$ als neues Basiselement

$$A_i' = A_i A_m^{x_i p^{\alpha_m - \alpha_i}} .$$

Nach (5) ergibt sich dann

$$(A_i')^{p^{\alpha_i}} = A_i^{p^{\alpha_i}} A_m^{x_i p^{\alpha_m}} = C^{a_i} C^{x_i a_m} = C^{a_i + x_i a_m} .$$

Wegen $a_m \neq 0$ kann man die linearen Kongruenzen

$$a_i' = a_i + x_i a_m \equiv 0 \pmod{p} \qquad (i \neq m)$$

lösen, so daß für die errechneten x_i-Werte alle $a_i' = 0$ werden. Die Basiselemente A_k mit $a_k = 0$ behalten wir bei, ebenso A_m. Nach

der Normierung der a_i stimmen die Ordnungen der Elemente $A_i (i \neq m)$ mit denen der Restklassen $A_i\mathfrak{C}$ überein:

$$\text{Ord } A_i = \text{Ord } A_i\mathfrak{C}.$$

Jetzt muß noch die Matrix (c_{ik}) durch geeignete Basisübergänge auf die gewünschte Form gebracht werden, ohne daß die normierten a_i sich ändern. Zu dem Zwecke ordnen wir die α_i der Größen nach:

$$\alpha_1 \leqq \alpha_2 \leqq \cdots \leqq \alpha_m < \alpha_{m+1} \leqq \alpha_{m+2} \leqq \cdots \leqq \alpha_s.$$

Ist kein $\alpha_i > \alpha_m$ vorhanden, so steht α_m an letzter Stelle. Die Basiselemente schreiben wir wieder ohne Striche: $A_1, A_2, \ldots, A_s$.

Der Basisübergang

$$A_i' = A_i^{x_i} \text{ mit } x_i \not\equiv 0 \pmod{p}$$

bedeutet für die Matrix (c_{ik}) Multiplikation der i-ten Zeile und i-ten Spalte mit x_i; denn es ist

$$A_i' A_k = A_i^{x_i} A_k = A_k A_i^{x_i} C^{x_i c_{ik}} = A A_i' C^{c'_{ik}},$$

also $$c'_{ik} = x_i c_{ik} \qquad (k = 1, 2, \ldots, s).$$

Hierbei ändern sich die Zahlen $a_i (i \neq m)$ nicht, da sie Null sind.

Die Transformation

$$A_k' = A_k A_i^{y_i} \qquad (k > i,\ y_i \text{ beliebig})$$

(man beachte die Anordnung der α_i) bedeutet für die Matrix (c_{ik}) Addition der mit y_i multiplizierten i-ten Zeile und i-ten Spalte zur k-ten Zeile und k-ten Spalte; denn es ist

$$A_k' A_l = A_k A_i^{y_i} A_l = A_k A_l A_i^{y_i} C^{y_i c_{il}}$$
$$= A_i A_k A_i^{y_i} C^{y_i c_{il} + c_{kl}} = A_l A_k' C^{c'_{kl}},$$

also $$c'_{kl} = y_i c_{il} + c_{kl} \qquad (l = 1, 2, \ldots, s).$$

Die Zahlen $a_i (i \neq m)$ sind auch nach dieser Transformation Null wegen

$$(A_k')^{p^{\alpha_k}} = A_k^{p^{\alpha_k}} A_i^{y_i p^{\alpha_k}} = C^{a_k} C^{y_i a_i p^{\alpha_k - \alpha_i}} = E.$$

Mit Hilfe dieser beiden Operationen formen wir die Matrix (c_{ik}) schrittweise um.

Sei c_{1i} die erste von Null verschiedene Zahl in der ersten Zeile von (c_{ik}), so erreichen wir durch den Basisübergang

$$A_n' = A_k A_i^{y_k} \qquad (k>i)$$

bei geeignetem y_k, daß alle $c_{1k}' = c_{1k} + y_k c_{1i} \equiv 0 \pmod{p}$ werden.

Durch $A_i^{x_i}$ mit $x_i c_{1i} \equiv 1 \pmod{p}$ kommt an die i-te Stelle in der ersten Zeile von (c_{ik}) die Zahl 1. Nach dieser Transformation hat die Matrix (c_{ik}) folgende Gestalt angenommen:

$$\begin{array}{cc} & \begin{array}{ccccccccc} & & & & (i) & & & & \end{array} \\ \begin{array}{c} \\ \\ \\ \\ (i) - \\ \\ \\ \\ \end{array} & \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & & & & \\ \vdots & & \cdot & & & & & \\ 0 & & & \cdot & & & & \\ 1 & & & & \cdot & & & \\ 0 & & & & & \cdot & & \\ \vdots & & & & & & 0 & \\ 0 & & & & & & & 0 \end{pmatrix} \end{array}$$

Sollten von Anfang an alle $c_{1i} = 0$ $(i = 1, 2, \ldots, s)$ sein, so bedeutet dies, daß das Element A_1 mit allen A_i vertauschbar ist. Ist dann $m \neq 1$, so kann man nach den Ausführungen auf S. 188 die zyklische Gruppe (A_1) direkt abspalten. Es ist zu beachten, daß $a_1 = 0$ ist für $m \neq 1$. Setzen wir $\mathfrak{M}$ als unzerlegbar voraus, was ohne Beschränkung der Allgemeinheit geschehen kann, da die Kommutatorgruppe direkt unzerlegbar ist, so können *nur* in der m-ten Zeile und Spalte lauter Nullen stehen. Nun multipliziere ich die erste Zeile mit $-c_{2i}$ und addiere sie zur zweiten. Dadurch tritt an die i-te Stelle in der zweiten Zeile eine Null, wodurch erreicht ist, daß bei den folgenden Transformationen die erste Zeile und Spalte unverändert bleiben. Jetzt kann man die Restmatrix, die durch Streichen der ersten Zeile und Spalte aus (c_{ik}) hervorgeht, genau so behandeln. Die Zahlen a_i $(i \neq m)$ sind nach Ausführung aller Transformationen Null geblieben.

Das Gesamtergebnis der Transformationen ist folgendes: Alle Zahlen a_i sind Null bis auf a_m, die Matrix (c_{ik}) enthält in jeder Zeile und Spalte nur eine von Null verschiedene Zahl ($+1$ oder -1), nur in der m-ten Zeile und Spalte *können* lauter Nullen stehen. In *diesem* Falle erhalten wir für $\mathfrak{M}$ das Schema (6) des Falles A., andernfalls das Schema (7) des Falles B.

Damit endlich die Zahl a_m noch den Wert 1 erhält, substituiere ich im Falle A.

$$A'_m = A_m^x \text{ mit } x a_m \equiv 1 \pmod{p};$$

hierbei ändern sich die anderen Zahlen nicht. Im Falle B. substituiere ich

$$S'_m = S_m^x \text{ mit } x a_m \equiv 1 \pmod{p}$$

und

$$R'_m = R_m^y \text{ mit } xy \equiv 1 \pmod{p};$$

dadurch wird auch hier a_m zu 1, und der Kommutator von S'_m und R'_m ist wieder C, an den übrigen Zahlen ändert sich dabei nichts.

Es ist damit alles bewiesen. Jeder unzerlegbaren Gruppe der hier behandelten Art kann ein Schema der Form (6) oder (7) zugeordnet werden.

Daß umgekehrt zu jedem vorgelegten Schema der Form (6) oder (7) auch eine Gruppe gehört, ist klar, da die beiden Bedingungen (3) und (4) erfüllt sind. Es bleibt noch zu zeigen, daß es zu jeder Gruppe auch *nur ein* Schema geben kann.

Zunächst ist leicht zu sehen, daß $\mathfrak{M}$ nicht gleichzeitig durch ein Schema der Form (6) und (7) gekennzeichnet werden kann; denn jedes Element X maximaler Ordnung, von dem eine geeignete Potenz die Kommutatorgruppe erzeugt, muß die Komponente S_m^x mit $(x, p) = 1$ bei Schema (7) enthalten, kann also nicht im Zentrum liegen, wie es bei dem Elemente D in Schema (6) der Fall ist.

Bevor ich den allgemeinen Beweis dafür führe, daß es zu jeder Gruppe nur ein Schema gibt, bringe ich ein Beispiel einer Gruppe, für die $t = 2$ ist, das in aller Deutlichkeit den Grund für die Invarianz der Zahlenpaare $\left\{ \begin{matrix} \varrho_i \\ \sigma_i \end{matrix} \right\}$ erkennen läßt.

Die Gruppe $\mathfrak{M}$ sei gekennzeichnet durch folgende beiden Schemata:

$$(8) \qquad \left.\begin{matrix} \\ \end{matrix}\right\} \text{ mit } \varrho_1 > \varrho_2 > \sigma_1 > \sigma_2 .$$

$$(9) \qquad \left.\begin{matrix} \\ \end{matrix}\right\}$$

Nach (8) läßt sich $\mathfrak{M}$ erzeugen durch

$$R_1^{p^{\varrho_1}} = E,\ R_2^{p^{\varrho_2}} = E,\ S_1^{p^{\sigma_1}} = E,\ S_2^{p^{\sigma_2}} = E,\ D^{p^\gamma - 1} = C,\ C^p = E,$$
$$R_1 S_1 = S_1 R_1 C,\ R_2 S_2 = S_2 R_2 C, \text{ sonst kommutativ;}$$

nach (9) dagegen durch

$$R_1'^{p^{\varrho_1}} = E\, R_2'^{p^{\varrho_2}},\ S_1'^{p^{\sigma_2}} = E,\ S_2'^{p^{\sigma_1}} = E,\ D'^{p^{\gamma-1}} = C',\ C'^p = E,$$
$$R_1' S_1' = S_1' R_1' C',\ R_2' S_2' = S_2' R_2' C', \text{ sonst kommutativ.}$$

Ist es nun möglich, nach dem Relationssystem (9) eine Basis mit dem Relationssystem (8) zu wählen? Ich setze an:

$$R_1 = R_1'^{r_{11}} R_2^{r_{12}} S_1'^{\bar{r}_{11}} S_2'^{\bar{r}_{12}},$$
$$R_2 = R_1'^{r_{21} p^{\varrho_1 - \varrho_2}} R_2'^{r_{22}} S_1'^{\bar{r}_{21}} S_2'^{\bar{r}_{22}},$$
$$S_1 = R_1'^{s_{11} p^{\varrho_1 - \sigma_1}} R_2'^{s_{12} p^{\varrho_2 - \sigma_1}} S_1'^{\bar{s}_{11}} S_2'^{\bar{s}_{12}},$$
$$S_2 = R_1'^{s_{21} p^{\varrho_1 - \sigma_2}} R_2'^{s_{22} p^{\varrho_2 - \sigma_2}} S_1'^{\bar{s}_{21}} S_2'^{\bar{s}_{22} p^{\sigma_1 - \sigma_2}}.$$

Wie ich nun auch die Zahlen r_{ik}, $\bar{r}_{ik}$, s_{ik}, $\bar{s}_{ik}$ wähle, stets gilt die Beziehung

$$R_2 S_2 = S_2 R_2;$$

denn jedes Element X^{p^x} liegt als p-te Potenz nach dem Ergebnis auf S. 187 im Zentrum. Es ist also unmöglich, nach Schema (9) eine Basis zu wählen, so daß $R_2 S_2 = S_2 R_2 C$ wird, wie Schema (8) erfordert. Die Schemata (8) und (9) kennzeichnen also nichtisomorphe Gruppen.

Den allgemeinen Beweis führe ich mit Hilfe der vollständigen Induktion nach der Gruppenordnung. Wenn $\mathfrak{M}$ durch zwei Schemata der Form (6) oder (7) gekennzeichnet wird, im Falle A. etwa durch

(10) $$\left[\begin{matrix} \varrho_1, \varrho_2, \ldots, \varrho_t \\ \sigma_1, \sigma_2, \ldots, \sigma_t \end{matrix} ; \gamma \right]_p$$

und

(10′) $$\left[\begin{matrix} \varrho_1', \varrho_2', \ldots, \varrho_{t'}' \\ \sigma_1', \sigma_2', \ldots, \sigma_{t'}' \end{matrix} ; \gamma' \right]_p,$$

im Falle B. durch

(11) $$\left[\begin{matrix} \varrho_1, \ldots, \varrho_m, \ldots, \varrho_t \\ \sigma_1, \ldots, \underline{\sigma_m}, \ldots, \sigma_t \end{matrix} \right]_p$$

und

(11′) $$\left[\begin{matrix} \varrho_1', \ldots, \varrho_{m'}', \ldots, \varrho_{t'}' \\ \sigma_1', \ldots, \underline{\sigma_{m'}'}, \ldots, \sigma_{t'}' \end{matrix} \right]_p,$$

so muß für (10) und (10′) zunächst $\gamma = \gamma'$ bzw. für (11) und (11′) $\sigma_m = \sigma_{m'}'$ sein; denn die Zahl γ bzw. σ_m gibt an, daß es in $\mathfrak{M}$ Elemente gibt, deren $p^{\gamma-1}$-te bzw. $p^{\sigma_m - 1}$-te Potenz die Kommutatorgruppe $\mathfrak{C}$ erzeugen, aber keine Elemente, deren p^{γ}-te bzw. p^{σ_m}-te Potenz $\mathfrak{C}$ erzeugen. Man kann dies kurz so ausdrücken:

γ bzw. σ_m gibt an, wie tief die Kommutatorgruppe $\mathfrak{C}$ in $\mathfrak{M}$ wurzelt.

Weiter muß in (10), (10′) bzw. (11), (11′) $t = t'$ sein; denn die Anzahl der Invarianten der abelschen Gruppe $\mathfrak{M}/\mathfrak{C}$ ist im Falle A. $2t + 1$ für $\gamma > 1$, $2t$ für $\gamma = 1$ bzw. $2t$ im Falle B.

Für den Fall B. muß auch noch $\varrho_m = \varrho'_{m'}$ sein. Um das zu beweisen, betrachte ich in $\mathfrak{M}$ den Komplex $\mathfrak{K}$, der aus allen Elementen K besteht, die die Ordnung p^{σ_m} haben und die Bedingung $(K) > \mathfrak{C}$ erfüllen. $\mathfrak{K}$ ist offenbar ein charakteristischer Komplex, d. h. er geht bei allen Automorphismen der Gruppe als Ganzes in sich über. Ferner betrachte ich alle Elemente aus $\mathfrak{M}$, deren Ordnungen $\leqq p^{\varrho_m}$ ist. Diese bilden, weil nach (5)

$$(A\,B)^p = A^p B^p$$

gilt, eine Gruppe $\mathfrak{U}(p^{\varrho_m})$, die eine charakteristische Untergruppe ist. Sie besteht nämlich aus allen Elementen, die eine Ordnungsrelation erfüllen. Bringen wir ein Element K aus $\mathfrak{K}$ auf die Form

$$K = \prod_{i=1}^{t} R_i^{r_i} \prod_{k=1}^{t} S_k^{s_k},$$

so muß $(s_m, p) = 1$ sein, und die übrigen Exponenten müssen gewisse leicht angebbare Bedingungen erfüllen, auf deren genaue Formulierung es hier nicht ankommt. Es gibt nun, wenn wir das Schema (11) zugrunde legen, kein Element K aus $\mathfrak{K}$, das mit *allen* Elementen aus $\mathfrak{U}(p^{\varrho_m})$ vertauschbar ist; denn $\mathfrak{U}(p^{\varrho_m})$ enthält R_m, das mit keinem K aus $\mathfrak{K}$ vertauschbar ist, weil jedes K die Komponente S_m^x mit $(x, p) = 1$ enthält, während R_m mit allen anderen Komponenten vertauschbar ist. Dagegen ist das Element S_m aus $\mathfrak{K}$ mit $\mathfrak{U}(p^{\varrho_m - 1})$ elementweise vertauschbar. Die Zahl ϱ_m ist mithin durch die Struktur der Gruppe eindeutig festgelegt (sie ist eine Gruppeninvariante), da sie durch $\mathfrak{K}$ und $\mathfrak{U}(p^{\varrho_m})$ bestimmt ist, die ihrerseits als charakteristische Komplexe durch die Struktur der Gruppe festgelegt sind. In (11), (11′) ist demnach $\varrho_m = \varrho'_{m'}$.

Ich gehe nun daran, durch Induktion zu beweisen, daß bei geeigneter Reihenfolge $\varrho_i = \varrho_i'$ und $\sigma_i = \sigma_i'$ ist.

Zu dem Zwecke ordne man die Zahlen ϱ_i und σ_i so, daß

$$\varrho_i \geqq \sigma_i, \quad \varrho_i \geqq \varrho_{i+1} \qquad (i = 1, 2, \ldots, t)$$

ist. Dabei kann die unterstrichene Zahl im Schema (11) in die erste Zeile treten. Bei gleichen ϱ_i sollen die σ_i in ihrer Größe die Reihenfolge bestimmen. Entsprechend ordne man die Zahlen in den gestrichenen Schemata.

Mit Rücksicht auf den Fall, daß bei der Induktion auch Gruppen mit direkten abelschen Faktoren auftreten werden, sind (10) und (11)

in folgender Weise zu erweitern:

$$\left[\begin{matrix}\varrho_1, \ldots, \varrho_t \\ \sigma_1, \ldots, \sigma_t\end{matrix}; \gamma; \tau_1, \ldots, \tau_n\right]_p, \tag{12}$$

$$\left[\begin{matrix}\varrho_1, \ldots, \varrho_m, \ldots, \varrho_t \\ \sigma_1, \ldots, \underline{\sigma_m}, \ldots, \sigma_t\end{matrix}; \tau_1, \ldots, \tau_n\right]_p. \tag{13}$$

Hierbei bedeuten $p^{\tau_1}, \ldots, p^{\tau_n}$ die Invarianten des direkten abelschen Faktors der durch (12) bzw. (13) gekennzeichneten Gruppe.

Man betrachte nun die charakteristische echte Untergruppe $\mathfrak{U}(p^{\omega-1})$, die aus allen und nur den Elementen aus $\mathfrak{M}$ besteht, deren Ordnungen $\leqq p^{\omega-1}$ sind, wobei p^ω die größte unter den in $\mathfrak{M}$ auftretenden Ordnungen der Elemente ist. Es möge nun

$$\varrho_1 = \varrho_2 = \cdots = \varrho_k > \varrho_{k+1}$$

gelten; dabei kann $k = t$ sein. Nach der Anordnung sind alle Zahlen $\sigma_i \leqq \varrho_k$. Weiter möge

$$\sigma_1 = \sigma_2 = \cdots = \sigma_i = \varrho_k \qquad (i \leqq k),$$
$$\sigma_i > \sigma_{i+1}$$

gelten, wobei $i = 0$ sein kann, d. h. es sind alle $\sigma_1, \sigma_2, \ldots, \sigma_i < \varrho_k$.

Zunächst sei $\gamma < \varrho_1$ vorausgesetzt. Dann wird die Untergruppe $\mathfrak{U}(p^{\omega-1})$ offenbar erzeugt durch die Elemente

$$R_1^p, S_1^p, \ldots, R_i^p, S_i^p, R_{i+1}^p, \ldots, R_k^p, R_{x\,(x>k)}, S_{y\,(y>i)}, D.$$

Da nach dem Ergebnis auf S. 187 die p-te Potenz eines Elementes im Zentrum liegt, lassen sich, wie oben ausgeführt wurde, die zyklischen Gruppen (R_i^p) und (S_i^p) direkt abspalten.

Es liegen aber auch die Elemente $S_{i+1}, \ldots, S_k$ im Zentrum von $\mathfrak{U}(p^{\omega-1})$; denn die Basiselemente $R_{i+1}, \ldots, R_k$, mit denen sie nicht vertauschbar sind, fehlen in $\mathfrak{U}(p^{\omega-1})$. Die Gruppe $\mathfrak{U}(p^{\omega-1})$ läßt sich daher durch folgendes Zahlenschema kennzeichnen:

$$\left[\begin{matrix}\varrho_{k+1}, \ldots, \varrho_t \\ \sigma_{k+1}, \ldots, \sigma_t\end{matrix}; \gamma; \varrho_1 - 1, \ldots, \varrho_k - 1; \sigma_1 - 1, \ldots, \sigma_i - 1, \sigma_{i+1}, \ldots, \sigma_k\right].$$

Da $\mathfrak{U}(p^{\omega-1})$ eine echte Untergruppe ist, so sind nach Induktionsvoraussetzung das ungestrichene und gestrichene Schema identisch, woraus durch Vergleich unmittelbar

$$\varrho_i = \varrho_i', \quad \sigma_i = \sigma_i' \qquad (i = 1, 2, \ldots, t)$$

folgt. Auch wenn $\varrho_1 \leqq \gamma$ sein sollte, ist der Beweis genau so zu führen. Damit ist alles gezeigt.

Bezeichnet man mit $\mathfrak{K}_p$ die direkt unzerlegbaren Gruppen, deren Kommutatorgruppenordnung eine Primzahl $p \neq 2$ ist und deren Kommutatorgruppe im Zentrum liegt, so erhält man die allgemeine Gruppe dieser Art, wenn man das direkte Produkt

$$\mathfrak{M} = \mathfrak{K}_p \times \mathfrak{A} \tag{14}$$

bildet, wobei $\mathfrak{A}$ eine beliebige endliche abelsche Gruppe ist. In (14) ist $\mathfrak{K}_p$ gewissermaßen der eindeutig bestimmte nichtabelsche Kern.

Versteht man unter $k(p^n)$ die Anzahl der Kerne der Ordnung p^n, unter $a(p^n)$ die Anzahl aller abelschen Gruppen der Ordnung p^n und unter $b(p^n)$ die Anzahl aller Gruppen der behandelten Art von der Ordnung p^n, so gilt wegen (14) die Relation

$$b(p^n) = \sum_{i=3}^{n} k(p^i)\, a(p^{n-i}). \tag{15}$$

Ich gebe nun ein Zahlenbeispiel, aus dem die Bedeutung der Zahlenschemata für Gruppenuntersuchungen zu ersehen ist. Es sollen alle Kerne der Ordnung p^5 angegeben werden. Man hat im Falle A.

$$\left[\begin{matrix}1\\1\end{matrix}; 3\right],\quad \left[\begin{matrix}2\\1\end{matrix}; 2\right],\quad \left[\begin{matrix}2\\2\end{matrix}; 1\right],\quad \left[\begin{matrix}3\\1\end{matrix}; 1\right],\quad \left[\begin{matrix}1,1\\1,1\end{matrix}; 1\right]$$

und im Falle B.

$$\left[\begin{matrix}1\\4\end{matrix}\right],\quad \left[\begin{matrix}2\\3\end{matrix}\right],\quad \left[\begin{matrix}3\\2\end{matrix}\right],\quad \left[\begin{matrix}1,1\\2,1\end{matrix}\right].$$

Es ist also $k(p^5) = 9$. Ebenso errechnet man

$$k(p^4) = 4,\ k(p^3) = 2,\ a(p^2) = 2,\ a(p) = 1;$$

mithin ist nach (15)

$$b(p^5) = 9 + 4 + 2 \cdot 2 = 17.$$

§ 2. Endliche Gruppen, deren Kommutatorgruppenordnung eine Primzahl ist und deren Kommutatorgruppe nicht im Zentrum liegt.[9])

Gegenüber den Untersuchungen des vorigen Paragraphen befreien wir uns zuerst von der Voraussetzung, daß die Kommutatorgruppe im Zentrum liegt. Die zu untersuchende Gruppe nenne ich wieder $\mathfrak{M}$. Die Faktorgruppe $\mathfrak{M}/\mathfrak{C}$, wo $\mathfrak{C}$ wieder die Kommutatorgruppe bezeichnen soll, sei als abelsche Gruppe vom Typus

$$[p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}].$$

9) Auch diese Gruppen sind zweistufig, vgl. A. Scholz, a. a. O. [2]).

A_i sei auch hier ein Repräsentant aus einer erzeugenden Restklasse des i-ten Faktors von $\mathfrak{M}/\mathfrak{C}$. Dann kann ich $\mathfrak{M}$ erzeugen durch die $s+1$ Elemente $A_1, A_2, \ldots, A_s$ und C mit Hilfe folgender definierender Relationen:

$$A_i^{p_i^{\alpha_i}} = C,\ A_i A_k = A_k A_i C^{c_{ik}},\ C^p = E,\ A_i^{-1} C A_i = C^{r_i} \qquad (i,k = 1,2,\ldots,s).$$

Damit durch diese Relationen auch wirklich eine Gruppe erzeugt wird, müssen die Zahlen p, p_i, α_i, c_{ik} und r_i folgende fünf Bedingungen erfüllen:

$$r_i^{p_i^{\alpha_i}} \equiv 1 \pmod p, \tag{16}$$

$$a_i(r_i - 1) \equiv 0 \pmod p, \tag{17}$$

$$c_{ij} + c_{ji} \equiv 0 \pmod p, \tag{18}$$

$$a_i(r_j - 1) + c_{ji}\frac{r_i^{p_i^{\alpha_i}} - 1}{r_i - 1} \equiv 0 \pmod p, \tag{19}$$

$$a_i(r_j - 1) + c_{ji} p_i^{\alpha_i} \equiv 0 \pmod p \text{ für } r_i - 1 \equiv 0 \pmod p, \tag{20}$$

$$c_{ij}(r_k - 1) + c_{ki}(r_j - 1) + c_{jk}(r_i - 1) \equiv 0 \pmod p \qquad (i \neq j, j \neq k, k \neq i). \tag{21}$$

Das Bestehen dieser Kongruenzen ist notwendig und hinreichend; denn sie erweisen sich als eine Spezialisierung der allgemeinen SCHREIERschen Bedingungen für den vorliegenden Fall. Um dies auszuführen, stelle ich durch folgende Tabelle die Bezeichnungen gegenüber:

SCHREIERsche Bezeichnung: A	B_i	A_i	$A_{i,j}$	A^{B_i}	$\mathfrak{A}$	n_i
Hier gebrauchte Bezeichnung: C	A_i	C^{a_i}	$C^{c_{ij}}$	$C^{A_i} = C^{r_i}$	$\mathfrak{C} = (C)$	$p_i^{\alpha_i}$

Der SCHREIERsche Satz, auf den wir uns stützen, lautet[10]):

Die Relationen

$$B_i^{-1} A B_i = A^{B_i},\ B_i^{n_i} = A_i,\ B_i B_j = B_j B_i A_{ij} \qquad (i \neq j)$$

zusammen mit den Relationen von $\mathfrak{A}$ definieren stets und nur dann eine Erweiterung von $\mathfrak{A}$ mit Hilfe der abelschen Gruppe vom Typus $[n_i]$, wenn in $\mathfrak{A}$ die Beziehungen gelten:

$$(A'A'')^{B_i} = A'^{B_i} A''^{B_i}, \tag{22}$$

$$\begin{pmatrix} A \\ A^{B_i} \end{pmatrix}^{n_i} = \begin{pmatrix} A \\ A_i^{-1} A A_i \end{pmatrix}, \tag{23}$$

$$A_i^{B_i} = A_i, \tag{24}$$

$$(A^{B_i})^{B_j} = A_{ij}^{-1} (A^{B_j})^{B_i} A_{ij}\ (A_{ij} A_{ji} = E), \tag{25}$$

$$A_i^{B_j} = A_i A_{ij}^{B_j^{n_i - 1} + \cdots + E}, \tag{26}$$

$$A_{ij}^{B_k} A_{kj} A_{ki}^{B_j} A_{ji} A_{jk}^{B_i} A_{ik} = E \qquad (i \neq j, j \neq k, k \neq i). \tag{27}$$

10) A. a. O. [7]), S. 180.

Im folgenden bedeutet der Pfeil $\rightarrow$ die Übertragung der SCHREIERschen Bedingungen (22) bis (27) in unsere Bezeichnung und Folgerungen, die zu den Bedingungen (16) bis (21) führen. Man beachte noch, daß umgekehrt mit (16) bis (21) auch zugleich die Bedingungen (22) bis (27) erfüllt sind.

Die Bedingung (22) besagt nichts, da die Kommutatorgruppe $\mathfrak{C}$ zyklisch ist. Die anderen Bedingungen liefern für unsere Gruppe folgende Relationen:

(23) ergibt

$$\binom{A}{A^{B_i}}^{n_i} = \binom{A}{A_i^{-1}\, A\, A_i} \rightarrow \binom{C}{C^{r_i}}^{p_i^{\alpha_i}} = \binom{C}{C^{-a_i}\, C\, C^{a_i}} = \binom{C}{C} \rightarrow C^{r_i p_i^{\alpha_i}} = C\,,$$

woraus (16) folgt.

(24) ergibt

$$A_i^{B_i} = A_i \rightarrow (C^{a_i})^{A_i} = C^{a_i} \rightarrow C^{a_i r_i} = C^{a_i},$$

woraus (17) folgt.

(25) ergibt

$$\begin{aligned}(A^{B_i})^{B_j} &= A_{ij}^{-1}(A^{B_j})^{B_i} A_{ij} \rightarrow (C^{A_i})^{A_j} \\ &= C^{-c_{ij}}(C^{A_j})^{A_i} C^{c_{ij}} \rightarrow C^{r_i r_j} = C^{-c_{ij}+r_j r_i + c_{ij}} = C^{r_j r_i}\,,\end{aligned}$$

$$A_{ij} A_{ji} = E \rightarrow C^{c_{ij}} C^{c_{ij}} = C^{c_{ij}+c_{ji}} = E\,,$$

woraus (18) folgt.

(26) ergibt

$$A_i^{B_j} = A_i A_{ij}^{B_i n_i - 1 + \cdots + E} \rightarrow (C^{a_i})^{A_j} = C^{a_i}(C^{c_{ij}})^{A_i^{p_i^{\alpha_i}-1+\cdots+E}} \rightarrow C^{a_i r_j}$$

$$= C^{a_i + c_{ij}\left(r_i^{p_i^{\alpha_i}-1} + \cdots + 1\right)} = C^{a_i + c_{ij}\frac{r_i^{p_i^{\alpha_i}}-1}{r_i - 1}}\,,$$

woraus (19) folgt. Für $r_i - 1 \equiv 0 \pmod{p}$ bekommt man daraus (20).

(27) ergibt

$$\begin{aligned}&A_{ij}^{B_k} A_{kj} A_{ki}^{B_j} A_{ji} A_{jk}^{B_i} A_{ik} = E \\ \rightarrow\ &(C^{c_{ij}})^{A_k} C^{c_{kj}} (C^{c_{ki}})^{A_j} C^{c_{ji}} (C^{c_{jk}})^{A_i} C^{c_{ik}} = E \\ \rightarrow\ &C^{c_{ij} r_k} C^{c_{kj}} C^{c_{ki} r_j} C^{c_{ji}} C^{c_{jk} r_i} C^{c_{ik}} = E\,,\end{aligned}$$

woraus (21) folgt.

Wie in § 1 gilt auch hier, daß jedes Gruppenelement M eindeutig in der Form

$$M = A_1^{x_1} A_2^{x_2} \cdots A_s^{x_s} C^y$$

darstellbar ist, wobei $x_i \bmod p_i^{\alpha_i}$ und $y \bmod p$ zu rechnen sind. Die Vereinfachung der Zahlensysteme der (c_{ik}) und a_i geht unter der Vor-

aussetzung, die für die folgenden Untersuchungen gemacht wird, daß nämlich die Kommutatorgruppe *nicht* im Zentrum liegt, viel weiter als im anderen Fall. Es gilt nämlich der bemerkenswerte und wichtige Satz:

Satz 1: *Man kann die Basiselemente A_i derart wählen, daß die Matrix (c_{ik}) die Nullmatrix wird, und daß alle $a_i = 0$ werden, d. h. daß sämtliche A_i untereinander vertauschbar und von der Kommutatorgruppe unabhängig sind, also* $\mathrm{Ord}(A_i) = \mathrm{Ord}(A_i\mathfrak{C})$ *gilt.*

Dieser Satz ist ein Spezialfall eines von A. SCHOLZ[11]) bewiesenen Satzes über zweistufige Gruppen.

In unserem Fall kann man aber den Satz 1 leichter nur mit Benutzung der SCHREIERschen Bedingungen beweisen.

Beweis: Unter den Zahlen r_k gibt es sicher eine, die $\not\equiv 1 \pmod p$ ist; denn andernfalls wäre jedes A_i mit C vertauschbar, und $\mathfrak{C}$ würde im Zentrum liegen. Dieses Element A_k (mit $r_k \not\equiv 1 \pmod p$) behalten wir als Basiselement bei. Alle übrigen A_i werden durch

$$A_i' = A_i C^{x_i} \qquad (i \neq k)$$

ersetzt. Es berechnet sich nun

$$\begin{aligned} A_i' A_k &= A_i C^{x_i} A_k = A_i A_k C^{x_i r_k} = A_k C_i^{c_{ik} + x_i r_k} \\ &= A_k A_i C^{x_i} C^{c_{ik} + x_i r_k - x_i} = A_k A_i' C^{c_{ik} + x_i (r_k - 1)}. \end{aligned}$$

Wählt man x_i $(i \neq k)$ so, daß es der Kongruenz

$$c_{ik}' = c_{ik} + x_i (r_k - 1) \equiv 0 \pmod p$$

genügt, was geht, da $r_k - 1 \not\equiv 0 \pmod p$ ist, so werden alle c_{ik}' für festes k und $i = 1, 2, \ldots, s$ zu Null. Aus den Bedingungen (21) und (18) folgt unmittelbar, daß dann auch die übrigen c_{im}' verschwinden. Dann besagen aber die Bedingungen (17) für $i = k$ und (19), (20) für $j = k$, daß bei dieser Wahl der Basis alle $a_i' = 0$ werden, was gezeigt werden sollte.

11) Hat die Gruppe die Gestalt $\mathfrak{G} = \sum S_\mu^{\alpha_\mu} T_\nu^{\alpha_\nu} \mathfrak{A}$, so kann man nach S. 346/47 der zitierten Scholzschen Arbeit erreichen, daß $S_\varkappa S_\lambda = S_\lambda S_\varkappa$, $\mathrm{Ord}(S_\varkappa) = \mathrm{Ord}(S_\mu \mathfrak{A})$ und $S_\mu T_\nu = T_\nu S_\mu$ wird. Setzen wir nun weiter voraus, daß $(\mathfrak{A}, \mathfrak{Z}) = 1$ ($\mathfrak{Z}$ = Zentrum) ist, wie es für unsere Gruppe $\mathfrak{M}$ der Fall ist, so folgt leicht $T_\mu T_\nu = T_\nu T_\mu$; denn aus $T_\mu T_\nu \neq T_\nu T_\mu$ würde folgen $T_\nu T_\mu = T_\mu T_\nu A$, also $A = T_\nu^{-1} T_\mu^{-1} T_\nu T_\mu$; es wäre also A mit S_λ vertauschbar, mithin A im Zentrum gelegen gegen unsere Voraussetzung $(\mathfrak{A}, \mathfrak{Z}) = 1$. Es bleibt noch zu zeigen, daß $\mathrm{Ord}(T_\mu) = \mathrm{Ord}(T_\mu \mathfrak{A})$ ist. Es sei $\mathrm{Ord}(T_\mu \mathfrak{A}) = t_\mu$, also $T_\mu^{t_\mu} = A_\mu$; wegen $S_\lambda T_\mu = T_\mu S_\lambda$ gilt auch $S_\lambda A_\mu = A_\mu S_\lambda$, und wegen $T_\mu T_\nu = T_\nu T_\mu$ gilt auch $T_\nu A_\mu = A_\mu T_\nu$, d. h. A_μ liegt im Zentrum, woraus wegen $(\mathfrak{A}, \mathfrak{Z}) = 1$ folgt $A_\mu = E$, d. h. $T_\mu^{t_\mu} = E$.

Aus diesen beiden Normierungsmöglichkeiten ergeben sich wichtige Folgerungen über die Struktur von $\mathfrak{M}$. Zunächst folgt zusammen mit (16), daß wir bezüglich der Primzahlen p_i die Fälle $(p_i, p-1) = 1$ ausschließen können; denn aus $(p_i, p-1) = 1$ würde $r_i = 1$ folgen, und die zyklische Gruppe (A_i) könnte direkt abgespalten werden. Man beachte dabei, daß alle $c_{ik} = 0$ und alle $a_i = 0$ sind. Setzen wir voraus, daß in $\mathfrak{M}$ solche Faktoren nicht vorhanden sind, so müssen sämtliche p_i Teiler von $p-1$ sein. Die Ordnung von $\mathfrak{M}$ ist demnach pm, wobei in m nur solche Primzahlen p_i aufgehen, die Teiler von $p-1$ sind. Da nach der Normierung alle Zahlen a_i und c_{ik} Null sind, ergibt sich als weitere wichtige Folgerung, daß die Struktur der Gruppe allein schon eindeutig festgelegt ist durch die Zahlen p, $p_i^{\alpha_i}$ und r_i $(i = 1, 2, \ldots, s)$. Die Zahl p wird nun eindeutig bestimmt durch die Struktur der Kommutatorgruppe $\mathfrak{C}$, während sich die Zahlen $p_i^{\alpha_i}$ eindeutig der Struktur von $\mathfrak{M}/\mathfrak{C}$ entnehmen lassen. Die Zahlen p und $p_i^{\alpha_i}$ sind also Gruppeninvarianten; dies gilt nicht von den Zahlen r_i, die sich ändern, wenn man von einer normierten Basis zur anderen übergeht.

Es gilt also, im folgenden einen gruppeninvarianten Ersatz für die r_i zu schaffen. Weiter werden sehr übersichtliche notwendige und hinreichende Bedingungen für die *direkte* Unzerlegbarkeit von $\mathfrak{M}$ entwickelt, und endlich wird ein einfaches, die Gruppe eindeutig kennzeichnendes Schema *invarianter* Zahlen angegeben, das eine leichte *Abzählung* aller in Frage stehenden *direkt* unzerlegbaren (damit auch aller zerlegbaren) Gruppen ermöglicht. Ich gebe dann noch kurz an, wie man zu einer anderen Art der Abzählung gelangt, wenn man Methoden anwendet, wie sie A. Scholz a. a. O.[2]) benutzt. Man kommt auf diesem Wege jedoch nicht zu einer Kennzeichnung der direkt unzerlegbaren Gruppen.

Unter den Primzahlen p_i mögen t gleiche vorkommen:

$$p_1 = p_2 = \cdots = p_t.$$

Von den übrigen p_i werde nur verlangt, daß sie von diesen ersten t Primzahlen verschieden sind. Unter ϱ_i soll die kleinste Zahl verstanden werden, die der Kongruenz

$$r_i^{p_i^{\varrho_i}} \equiv 1 \pmod{p}$$

genügt. $p_i^{\varrho_i}$ ist demnach die Ordnung der durch r_i bestimmten Restklasse innerhalb der Gruppe der zu p teilerfremden Restklassen. Nach (16) ist $\alpha_i \geqq \varrho_i$. Wir setzen

$$\alpha_i - \varrho_i = \sigma_i \qquad (i = 1, 2, \ldots, s).$$

Dann gilt

Satz 2: *Die Gruppe $\mathfrak{M}$ ist dann und nur dann direkt unzerlegbar, wenn nachstehende Bedingungen erfüllt sind:*

$$\varrho_1 > \varrho_2 > \cdots > \varrho_t > 0, \tag{28}$$

$$\sigma_1 > \sigma_2 > \cdots > \sigma_t \geqq 0. \tag{29}$$

Beweis: Für $\varrho_i = 0$ wäre $r_i = 1$, und die zyklische Gruppe (A_i) ließe sich direkt abspalten. Wir ordnen nun die ϱ_i der Größe nach:

$$\varrho_1 \geqq \varrho_2 \geqq \cdots \geqq \varrho_t.$$

Sollten zwei ϱ_i einander gleich sein, so bestimmen die σ_i die Reihenfolge. Nach dieser Anordnung ist die aus den Potenzen von r_{i+1} bestehende zyklische Restklassengruppe (r_{i+1}) Untergruppe von (r_i), da die Gruppe der zu p teilerfremden Restklassen zyklisch ist und Ord $(r_{i+1}) = p_{i+1}^{\varrho_{i+1}}$ enthalten ist in Ord $(r_i) = p_i^{\varrho_i}$. Man beachte, daß $p_i = p_{i+1}$ und $\varrho_i \geqq \varrho_{i+1}$ ist. Es ist also

$$r_{i+1} \equiv r_i^{x p_i^{\varrho_i - \varrho_i + 1}} \pmod{p} \text{ mit } (x, p_i) = 1.$$

Wähle ich statt A_i das Basiselement $A_i' = A_i^x$, so geht r_i über in $r_i' = r_i^x$. Ich kann also bei dieser Wahl der Basiselemente annehmen, daß $x = 1$, also

$$r_{i+1} = r_i^{p_i^{\varrho_i - \varrho_i + 1}}$$

ist. Sollte nun $\varrho_i = \varrho_{i+1}$ sein, so gehe man zu dem neuen Basiselement

$$A_i' = A_i A_{i+1}^{-1}$$

über. Dieses Element ist mit C vertauschbar; denn es ist

$$A_i'^{-1} C A_i' = A_{i+1} A_i^{-1} C A_i A_{i+1}^{-1} = C^{r_i r_{i+1}^{-1}} = C,$$

da wegen $\varrho_i = \varrho_{i+1}$ gilt $r_i = r_{i+1}$.

Weiter ist $$A_i'^{p_i^{\alpha_i}} = A_i^{p_i^{\alpha_i}} A_{i+1}^{-p_i^{\alpha_i}} = E.$$

Beim Rechnen ist zu beachten, daß die A_i unter sich vertauschbar sind. Die zyklische Gruppe (A_i) bildet daher einen direkten Faktor gegen die Voraussetzung.

Sollte $\sigma_i \leqq \sigma_{i+k}$ sein, so wähle man als neues Basiselement

$$A'_{i+k} = A_{i+k} A_i^{-p_i^{\varrho_i - \varrho_{i+k}}}.$$

A'_{i+k} ist mit C vertauschbar; denn es ist

$$A_{i+k}^{\prime -1} C A' = A_i^{p_i^{\varrho_i - \varrho_{i+k}}} A_{i+k}^{-1} C A_{i+k} A_i^{-p_i^{\varrho_i - \varrho_{i+k}}}$$
$$= C^{r_{i+k} r_i^{-p_i^{\varrho_i - \varrho_{i+k}}}} = C^{r_{i+k} r_{i+k}^{-1}} = C,$$

da $r_{i+k} = r_i^{p_i^{\varrho_i - \varrho_{i+k}}}$ ist. Weiter ist

$$A_{i+k}^{\prime p_i^{\alpha_{i+k}}} = A_{i+k}^{p_i^{\alpha_{i+k}}} A_i^{-p_i^{\varrho_i + \sigma_{i+k}}} = E.$$

Die zyklische Gruppe (A'_{i+k}) läßt sich daher wieder direkt abspalten.

Für die ersten t gleichen Primzahlen ist damit die Notwendigkeit von (28) und (29) für die Unzerlegbarkeit der Gruppe bewiesen. Für die nächsten t' gleichen Primzahlen $p_1' = p_2' = \cdots = p_{t'}'$ können wir genau so verfahren usw.

Im folgenden werden die gleichen Primzahlen auch gleich bezeichnet, also

$$p_1 = p_2 = \cdots = p_t = q,$$
$$p_1' = p_2' = \cdots = p_{t'}' = q',$$
$$\cdots\cdots\cdots$$

Jede direkt unzerlegbare Gruppe läßt sich daher nach den bisherigen Ausführungen durch folgendes Zahlenschema kennzeichnen:

$$\mathfrak{M}: \left.\begin{array}{lll} q: & \varrho_1, \sigma_1; & \varrho_2, \sigma_2; \cdots; \varrho_t, \sigma_t \\ q': & \varrho_1', \sigma_1'; & \varrho_2', \sigma_2'; \cdots; \varrho_{t'}', \sigma_{t'}' \\ & \cdots\cdots\cdots & \end{array}\right\}_p \qquad (q \neq q', \cdots),$$

wobei nur folgende Bedingungen erfüllt sein müssen:

(30) $\quad \varrho_1 > \varrho_2 > \cdots > \varrho_t > 0,\ \varrho_1' > \varrho_2' > \cdots > \varrho_{t'}' > 0, \cdots,$

(31) $\quad \sigma_1 > \sigma_2 > \cdots \geqq \sigma_t \geqq 0,\ \sigma_1' > \sigma_2' > \cdots > \sigma_{t'}' \geqq 0, \cdots,$

(32) $\quad p \equiv 1 \pmod{q^{\varrho_i}},\ p \equiv 1 \pmod{q'^{\varrho_{i'}}}, \cdots.$

Das Schema ist so zu verstehen: Die Gruppe $\mathfrak{M}$ hat die Erzeugenden $A_i, A_i', \ldots, C$ mit den definierenden Relationen

$$A_i^{q^{\varrho_i + \sigma_i}} = E,\ A_i^{\prime q'^{\varrho_{i'} + \sigma_{i'}}} = E, \cdots, \qquad (q \neq q', \cdots),$$
$$A_i^{-1} C A_i = C^{r_i},\ A_i^{\prime -1} C A_i' = C^{r_{i'}}, \ldots,$$
$$\text{sonst kommutativ},\ C^p = E,$$
$$\mathrm{Ord}(r_i) = q^{\varrho_i},\ \mathrm{Ord}(r_i') = q'^{\varrho_{i'}}, \cdots.$$

Daß es zu jedem vorgegebenen Schema eine Gruppe gibt, folgt aus dem SCHREIERschen Satz. Es bleibt noch zu zeigen, daß es zu jedem Schema auch nur eine Gruppe geben kann und daß sie direkt unzerlegbar ist. Ich führe den ersten Teil des Beweises so, daß ich zeige, daß die Zahlen des Schemas eindeutig durch die Struktur der Gruppe festgelegt sind (Gruppeninvariante).

Das Auftreten der Zahlen q, ϱ_i, σ_i im Schema bedeutet, daß es in $\mathfrak{M}$ ein Element A_i gibt, das erstens die Ordnung $q^{\varrho_i+\sigma_i}$ besitzt und zweitens in $\mathfrak{C}$ einen Automorphismus der Ordnung q^{ϱ_i} erzeugt; denn es ist

$$A_i^{q^{\varrho_i}+\sigma_i} = E \text{ und } A_i^{-1} C A_i = C^{r_i} \text{ mit } r_i^{q^{\varrho_i}} \equiv 1 \pmod{p}.$$

Jedes Element M von der Ordnung $q^{\varrho_i+\sigma_i}$ besitzt die Form

$$M = \prod_{k=1}^{i-1} A_k^{x_k q^{\varrho_k}+\sigma_k-\varrho_i-\sigma_i} A_i^{x_i} \prod_{k=i+1}^{t} A_k^{x_k}.$$

Soll der durch M in $\mathfrak{C}$ erzeugte Automorphismus außerdem die Ordnung q^{ϱ_i} besitzen, so muß $x_i \not\equiv 0 \pmod{q}$ sein; denn die anderen Faktoren von M erzeugen, wie x_k auch gewählt sein mag, Automorphismen niedrigerer Ordnung in $\mathfrak{C}$. Man beachte die Bedingungen (30) und (31). Die Zahlen q, ϱ_i und σ_i sind also durch die Struktur von $\mathfrak{M}$ bestimmt, sind demnach Gruppeninvarianten.

Jetzt folgt auch leicht die Unzerlegbarkeit von $\mathfrak{M}$. Da $\mathfrak{M}$ eine direkt unzerlegbare Kommutatorgruppe besitzt, ist bei einer Zerlegung von $\mathfrak{M}$ in zwei Faktoren der eine abelsch. Ließe sich nun eine zyklische Gruppe der Ordnung q^x abspalten, so müßten nach bekannten Sätzen q^x unter den Invarianten der abelschen Gruppe $\mathfrak{M}/\mathfrak{C}$ vorkommen, also gleich einem der $q^{\varrho_i+\sigma_i}$ sein; dann wäre aber $\varrho_i = 0$, was nicht sein kann, da q, ϱ_i, σ_i gruppeninvariant sind.

Die Invarianten von $\mathfrak{M}/\mathfrak{C}$ sind

$$\mathfrak{M}/\mathfrak{C}: \quad \begin{matrix} q^{\varrho_1+\sigma_1}, & q^{\varrho_2+\sigma_2}, & \cdots, & q^{\varrho_t+\sigma_t}, \\ q'^{\varrho_1'+\sigma_1'}, & q'^{\varrho_2'+\sigma_2'}, & \cdots, & q'^{\varrho_{t'}'+\sigma_{t'}'}, \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \end{matrix}$$

Die Invarianten des Zentrums lassen sich leicht errechnen zu

$$\mathfrak{Z}: \quad \begin{matrix} q^{\varrho_2+\sigma_1}, & q^{\varrho_3+\sigma_2}, & \cdots, & q^{\varrho_t+\sigma_{t-1}}, & q^{\sigma_t}, \\ q'^{\varrho_2'+\sigma_1'}, & q'^{\varrho_3'+\sigma_2'}, & \cdots, & q'^{\varrho_{t'}'+\sigma_{t'-1}'}, & q'^{\sigma_{t'}'}, \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \end{matrix}$$

Auch hieraus folgt unmittelbar die Invarianz der Zahlen q, ϱ_i, σ_i, q', ϱ_i', σ_i', ...

Es ergibt sich als

Folgerung: *Die Struktur von* $\mathfrak{M}$ *ist eindeutig bestimmt durch die Struktur von* $\mathfrak{C}$, $\mathfrak{M}/\mathfrak{Z}$ *und* $\mathfrak{Z}$.

Bezeichnen wir wieder wie in § 1 die unzerlegbaren unter den behandelten Gruppen mit $\mathfrak{K}_p$, so erhält man die allgemeinen Gruppen in der Form

$$\mathfrak{M} = \mathfrak{K}_p \times \mathfrak{A}, \tag{33}$$

wobei $\mathfrak{A}$ eine beliebige abelsche Gruppe ist. $\mathfrak{K}_p$ ist auch hier wie in (14) der eindeutig bestimmte unzerlegbare Kern in $\mathfrak{M}$.

Die verschiedenen Kerne $\mathfrak{K}_p$ findet man, indem man die verschiedenen unter den Primfaktoren von $p-1$ herausgreift und die Bedingungen (30), (31) und (32) berücksichtigt.

Ich gebe nun in ganz groben Umrissen an, wie man mit den in der Scholzschen Arbeit a. a. O.[2]) entwickelten Methoden zu einer anderen Gruppenabzählung gelangt.

Die Transformation, die $\mathfrak{M}/\mathfrak{C}$ in (C) bewirkt, definiert einen abelschen Charakter j in $\mathfrak{M}$ der Ordnung b, wenn b das kleinste gemeinschaftliche Vielfache der Transformationsexponenten in (C) bedeutet, also $r_i^b \equiv 1 \pmod{p}$ für alle r_i ist.

Die Gesamtheit aller Elemente H, die C invariant lassen ($H^{-1} C H = C$), bilden eine charakteristische Untergruppe $\mathfrak{H}$, deren Faktorgruppe $\mathfrak{M}/\mathfrak{H}$ zyklisch von der Ordnung b ist. Weiter ist b ein Teiler von $p-1$. Die abelsche Gruppe $\mathfrak{H}$ zerfällt direkt in

$$\mathfrak{H} = \mathfrak{C} \times \mathfrak{Z} \qquad (\mathfrak{Z} = \text{Zentrum von } \mathfrak{M}).$$

Demnach ist $\mathfrak{M}$ das *relative* Produkt der beiden Faktorgruppen $\mathfrak{M}/\mathfrak{C}$ und $\mathfrak{M}/\mathfrak{Z}$ über $\mathfrak{M}/\mathfrak{H}$. Nun ist aber das Kompositionsgesetz eines relativen Produktes durch die Kompositionsgesetze seiner Faktoren schon eindeutig bestimmt. Um die Struktur[12]) der Gruppe $\mathfrak{M}$ eindeutig festzulegen, genügt es daher in unserem Falle, die Strukturen von $\mathfrak{C}$ und $\mathfrak{M}/\mathfrak{C}$ und die Einbettung der zyklischen Gruppe $\mathfrak{M}/\mathfrak{H}$ in der abelschen Gruppe $\mathfrak{M}/\mathfrak{C}$ oder, was auf dasselbe hinauskommt, die Struktur von $\mathfrak{Z}$ vorzugeben. Damit haben wir auch hier noch einmal die oben ausgesprochene Folgerung, daß nämlich die Struktur von $\mathfrak{M}$ eindeutig durch die der Faktorgruppe $\mathfrak{M}/\mathfrak{C}$, der Kommutatorgruppe $\mathfrak{C}$ und des Zentrums $\mathfrak{Z}$ festgelegt ist.

12) Vgl. a. a. O. [2]), S. 339.

Zugleich ist jetzt die Abzählung aller fraglichen Gruppen $\mathfrak{M}$ der Ordnung mp (vgl. S. 201) auf folgende Aufgaben über abelsche Gruppen zurückgeführt: Es ist die Gesamtheit aller Typen von Einbettung einer zyklischen Gruppe der Ordnung b, wo b ein Teiler von $p-1$ ist, als Faktorgruppe in eine abelsche Gruppe des Typus $[p_1, p_2, \ldots, p_s]$ aufzustellen.

Übersichtlicher gestaltet sich die Abzählung, wenn wir $\mathfrak{M}/\mathfrak{C}$ in Primärgruppen zerlegen:

$$M/\mathfrak{C} = \mathfrak{Q}_1 \times \mathfrak{Q}_2 \times \cdots \times \mathfrak{Q}_t \ (\text{Ord}\ \mathfrak{Q}_i = q_i^{\varepsilon_i}).$$

Entsprechend spaltet sich dann

$$b = q_1 q_2 \cdots q_t.$$

Für die einzelnen q_i ist danach die Aufstellung aller fraglichen Gruppen der Ordnung $q_i^{\varepsilon_i} p$ identisch mit der abelschen Aufgabe, für $k = 1, 2, \ldots, \beta_i$, wo $q_i^{\beta_i}$ die höchste in $p-1$ aufgehende Potenz von q_i ist, die Gesamtheit aller Typen von Einbettung einer zyklischen Gruppe der Ordnung $q_i^{\varkappa}$ als Faktorgruppe in eine abelsche Gruppe der Ordnung $q_i^{\varepsilon_i}$ aufzustellen. Zu jedem Typus gehört dabei genau eine der gesuchten Gruppen $\mathfrak{M}$. Diese Aufgabe läßt eine leichte Abzählung zu, wobei die Abzählungen für die einzelnen q_i unabhängig kombiniert werden können. Diese Abzählung gestattet aber nicht, die direkt unzerlegbaren Kerne $\mathfrak{K}_p$ in (33) zu erkennen.

Die Untersuchungen von § 1 und § 2 zusammen liefern folgendes

Ergebnis: *Man findet jede endliche Gruppe, deren Kommutatorgruppenordnung eine Primzahl $p \neq 2$ ist, indem man zuerst die Kerne $\mathfrak{K}_p$ nach § 1 sucht, deren Kommutatorgruppe im Zentrum liegt, dann nach § 2 die übrigen Kerne $\mathfrak{K}_p'$ feststellt, deren Kommutatorgruppe nicht im Zentrum liegt, und jedesmal die auffüllenden direkten abelschen Faktoren hinzusetzt.*

Der Fall, daß die Kommutatorgruppenordnung $p = 2$ ist, der in § 2 offenbar nicht in Betracht kommt, weil eine Gruppe der Ordnung 2 nur den identischen Automorphismus gestattet ($A_i^{-1} C A_i = C$), weist eine andere Struktur als die in § 1 untersuchten Gruppen auf. Für $p = 2$ gilt nämlich nicht die Relation (5). Bei der Untersuchung dieser Gruppen, die aber nicht in dieser Arbeit erfolgen soll, spielen die Quaternionengruppe und die Diedergruppe für das Quadrat eine entscheidende Rolle.

Die Ergebnisse des § 1 lassen sich in leichter Weise auf sämtliche Gruppen, deren Kommutatorgruppe im Zentrum liegt und eine *quadratfreie* Ordnung besitzt, erweitern, was zum Abschluß geschehen soll.

Nach bekannten gruppentheoretischen Sätzen zerfallen die angegebenen Gruppen direkt und eindeutig in p-Gruppen. Die zu behandelnde Gruppe $\mathfrak{M}$ zerfällt also in

$$\mathfrak{M} = \mathfrak{U}_1 \times \mathfrak{U}_2 \times \cdots \times \mathfrak{U}_t,$$

wobei $$\operatorname{Ord}(\mathfrak{U}_i) = p_i^{\mu_i} \qquad (p_i \neq p_k \text{ für } i \neq k)$$

ist. Bekanntlich zerfällt dann auch die Kommutatorgruppe in

$$\mathfrak{C} = \mathfrak{C}_1 \times \mathfrak{C}_2 \times \cdots \times \mathfrak{C}_t,$$

wobei $\mathfrak{C}_i$ die Kommutatorgruppe von $\mathfrak{U}_i$ ist. Setze ich $\operatorname{Ord}(\mathfrak{C}_i) = p_i^{\gamma_i}$, so muß, da die Ordnung von $\mathfrak{C}$ nach Voraussetzung quadratfrei ist, $\gamma_i = 1$ oder $\gamma_i = 0$ sein. Für $\gamma_i = 1$ ist $\mathfrak{U}_i$ eine Gruppe, wie wir sie in § 1 behandelt haben; denn $\mathfrak{C}_i$ liegt offenbar im Zentrum von $\mathfrak{U}_i$. Ist $\gamma_i = 0$, so ist $\mathfrak{U}_i$ abelsch, womit die Erweiterung dargetan ist.

Lebenslauf

Am 30. Januar 1909 bin ich, Heinz Liermann, als zweiter Sohn des Volksschullehrers Gustav Liermann in Altlülfitz, Kr. Belgard in Pommern, geboren. Ich bin evangelischer Konfession. Bis Ostern 1928 besuchte ich das humanistische Gymnasium in Belgard, das ich mit dem Reifezeugnis verließ. Darauf studierte ich ein Jahr in Greifswald Mathematik, Physik und Chemie. Anschließend studierte ich drei Jahre in Halle dieselben Fächer, wo ich Ostern 1933 die wissenschaftliche Prüfung für das Lehramt an höheren Schulen mit dem Gesamtergebnis „mit Auszeichnung" bestand. Nach anschließender zweijähriger Vorbereitungstätigkeit legte ich im Februar 1935 in Berlin die pädagogische Prüfung für das Lehramt an höheren Schulen ab. Von meinem sechsten Semester ab war ich 3 Jahre hindurch als wissenschaftliche Hilfskraft am mathematischen Seminar in Halle tätig. Vom 1. November 1935 bis 1. Oktober 1936 arbeitete ich als Assistent für Finanz- und Wirtschaftsmathematik an der Technischen Hochschule in Berlin. Vom 1. Mai 1937 bis 1. August 1937 betätigte ich mich am geodätischen Institut in Potsdam bei der rechnerischen Auswertung von Erdschweremessungen im Rahmen des Vierjahresplanes.

Herrn Dr. Neiss spreche ich an dieser Stelle für die Unterstützung bei der Abfassung der Arbeit meinen herzlichsten Dank aus.